

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION  
International Bureau

## INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

<b>(51) International Patent Classification <sup>6</sup> :</b> <b>H04L 12/26, 12/24</b>	<b>A1</b>	<b>(11) International Publication Number:</b> <b>WO 99/18695</b> <b>(43) International Publication Date:</b> 15 April 1999 (15.04.99)
<b>(21) International Application Number:</b> PCT/IL98/00475 <b>(22) International Filing Date:</b> 28 September 1998 (28.09.98) <b>(30) Priority Data:</b> 121898 7 October 1997 (07.10.97) IL <b>(71) Applicant (for all designated States except US):</b> ATTUNE NETWORKS LTD. [IL/IL]; Suite 113, Jabotinsky Street 33, 52511 Ramat Gan (IL). <b>(72) Inventors; and</b> <b>(75) Inventors/Applicants (for US only):</b> CIDON, Israel [IL/IL]; Morad Hayasmin Street 10, 34762 Haifa (IL). SIDI, Moshe [IL/IL]; Haim Hazaz Street 1/2, 34996 Haifa (IL). <b>(74) Agents:</b> COLB, Sanford, T. et al.; Sanford T. Colb & Co., P.O. Box 2273, 76122 Rehovot (IL).		<b>(81) Designated States:</b> AL, AM, AT, AT (Utility model), AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, CZ (Utility model), DE, DE (Utility model), DK, DK (Utility model), EE, EE (Utility model), ES, FI, FI (Utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Utility model), SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).  Published <i>With international search report.</i>
<b>(54) Title: FAULT LOCATION AND PERFORMANCE TESTING OF COMMUNICATION NETWORKS</b>		
<b>(57) Abstract</b>  A method and apparatus for testing a network having a plurality of nodes (24). The method includes sending commands to one or more traffic agents (60) connected to the network (20) and to at least one network management agent (70) coupled to a respective node (24) of the network (20), transmitting data from at least one of the traffic agents (60) over the network responsive to the commands, determining network information at the at least one network management agent (70) responsive to the commands and to transmission of the data through the respective node, and receiving and evaluating the network information to assess a state of the network.		

FAULT LOCATION AND PERFORMANCE TESTING OF COMMUNICATION  
NETWORKS

**FIELD OF THE INVENTION**

The present invention relates generally to communication networks, and specifically to  
5 testing and fault discovery in communication networks.

**BACKGROUND OF THE INVENTION**

Communication networks are in wide use in many technological fields including distributed computing, data exchange and telecommunication applications. Communication networks generally include a plurality of nodes, such as bridges, LAN switches, routers, cross-  
10 connections and telephone switches. The networks further include communication links, such as cables, point-to-point radio connections and optical fibers, which connect the nodes. The networks also include ports, generally within some of the nodes, for attaching external devices such as computers, terminals, handsets, and multiplexers referred to as end-points (or hosts).

Networks are becoming increasingly complex, especially due to their increasing speeds  
15 of operation, the number of units interconnected by a network and the formation of large networks from different types of sub-networks. In addition, the networks may transmit concurrently various types of data such as text, voice, video and other multimedia files. In order to allow for these different types of data, some networks are designed to provide different amounts of bandwidth and different levels of quality of service.

20 A major issue with newly deployed and existing communication networks is testing and trouble-shooting, i.e., checking whether the network is operating according to its specifications and, if not, determining the cause of the network's inadequate performance (for example, the identity of a faulty unit).

Simulators such as "BONeS," produced by Cadence, San Jose, California, and  
25 "OPNET," produced by MIL3, Washington, DC, allow creation of models of a network, and subsequent testing of the network based on these models. An operator provides the simulator with a map of the network, which includes its components, specifications and expected data traffic patterns. The simulator provides performance estimations of the entire network, together with performance estimations of the network under various constraints, such as a non-  
30 operating node or link. Such performance estimation under constraints is referred to as "what-if" analysis. However, simulators do not usually cover all aspects of the simulated networks and are limited in the network size which may be simulated. In addition, simulators are able to

## SUMMARY OF THE INVENTION

It is an object of some aspects of the present invention to provide methods and apparatus for locating faults within communication networks.

It is another object of some aspects of the present invention to provide methods and  
5 apparatus for evaluation of the performance of communication networks.

It is yet another object of some aspects of the present invention to provide methods and apparatus for automatic detection of faults in a communication network.

It is still another object of some aspects of the present invention to provide methods and apparatus for systematic evaluation of the performance of a communication network.

10 It is still another object of some aspects of the present invention to provide methods and apparatus for evaluation of the performance of a communication network from a single central site.

In preferred embodiments of the present invention, a distributed testing system for evaluating and/or testing a communication network comprises a plurality of traffic agents  
15 coupled to nodes and/or hosts of the network. The traffic agents act as artificial users of the network by, for example, transmitting and receiving packets of data, establishing connections, and determining traffic statistics. The testing system further comprises one or more network management (NM) agents coupled to nodes (and possibly to hosts) of the network, which provide information on the interior state of the network. The network management agents  
20 preferably monitor the state of the node to which they are coupled, and monitor and possibly copy the traffic that passes through the node. The network management agents preferably also accept commands to configure the node to which they are coupled in terms of its communication abilities.

The testing system further comprises a testing center which conducts tests of the  
25 network. The testing center controls the operations of the traffic agents and NM agents by sending them commands or groups of commands, referred to herein as subscripts. In response to the commands, the traffic agents and/or NM agents perform actions and generate reports relating to the network and the traffic therethrough and send the reports to the testing center. The testing center uses the reports from the agents to determine additional tests to be  
30 performed and/or to evaluate the state of the network and generate test results which are provided to an operator. Preferably, the testing center stores a plurality of pre-written sets of instructions, referred to herein as scripts, each of which is directed to conduct a specific test session.

transmit digital data, preferably in packets or bit streams, and/or transmit connection establishment requests destined for other network endpoints. The traffic generators generate and transmit the digital data according to commands received from the testing center. Such commands may include times of transmission, as well as amounts of data to be transmitted in  
5 definite or statistical terms. The digital data transmitted as payload may include random bits and/or repetitions of predetermined sequences of data, useful in testing the network.

Alternatively or additionally, the digital data include test information which is useful in analysis of the state of the network. Such information may include, for example, the exact transmission time of the digital data, a sequence number of the data in a packet stream, and  
10 information regarding the stream including the packet, such as the number of blocks in the stream, the identity of the start and end packets of the stream, and information regarding the nature and generation timing of future data in the stream. Optionally, the traffic generators transmit data using multicasting and/or broadcasting, as is known in the art.

In some preferred embodiments of the present invention, the traffic generators can also  
15 communicate with hosts of the network which do not form part of the testing system. Such traffic generators preferably emulate digital data generated in accordance with standard protocols of various network applications, such as electronic mail (SMTP), database query (SQL), ping, TCP, UDP, HTTP, etc.

Preferably, the traffic agents further include one or more traffic analyzers, which receive  
20 data packets or signals from the network and measure and determine the nature, timing and contents of the data according to commands from the testing center. The traffic analyzers may receive all data passing over the network to the port to which they are connected, or only data which were generated by traffic generators. Preferably, the traffic analyzers accept requests for connection establishment and measure and determine the behavior of connections established  
25 with the analyzer or with endpoints coupled thereto.

The traffic analyzers generate and send to the testing center reports describing features of the received data. These reports are used by the testing center to evaluate the network. The contents of these reports, as well as their number and form, are in accordance with commands from the testing center. The traffic analyzers may generate a single report after an entire test  
30 session or a part of the test session, or they may generate multiple reports, periodically or otherwise. Preferably, the traffic analyzers receive only specific data and/or generate the test reports regarding only specific data identified in the commands. Such specific data may include data which conform with one or more specific protocols, originate from specific traffic

In some preferred embodiments of the present invention, the NM agents may alter the configuration of the network, and preferably have the total control of the network nodes, as is known in the art. For example, the NM agents preferably activate and/or deactivate links of the network. Additionally, the NM agents may control communication properties of the nodes, such as the service levels, operational status and priorities assigned to different data packets passing through the nodes. The NM agents are also preferably able to configure nodal tables, addresses and policies.

Preferably, the NM agents have capturing, filtering and/or masking capabilities to identify, store and/or count data packets with specific characteristics. Further preferably, the NM agents also have full monitoring capabilities for traffic that passes through their respective nodes. The monitoring preferably includes, but is not limited to, counting and/or measuring data packets according to one or more parameters, such as their source, destination, application type or a general bit pattern included in the packets. Alternatively or additionally, the monitoring includes copying and/or capturing individual data packets according the one or more parameters. Preferably, in connection-oriented networks, the NM agents identify, monitor and/or measure call establishment requests and setups that pass through the node to which they are coupled.

Preferably, the network management agents generate reports describing the traffic passing through their respective nodes. These reports are generated according to commands received from the testing center. The NM agents may generate a single report at the end of a test session (or a part thereof) or may generate multiple reports during the test sessions. Preferably, such reports are generated according to network management standards known in the art.

Preferably, all of the commands to be performed by each of the traffic agents during a single test session are sent to the agents prior to the test session. Alternatively, the test session includes a plurality of steps and subscripts that are sent to the agents during the test session, generally between execution of some or all of the steps of the session. Some of the subscripts are preferably generated responsive to reports received by the testing center from traffic agents and network management agents during prior steps of the test session.

In some preferred embodiments of the present invention, one or more of the embedded traffic agents operates in association with a network management agent coupled to the same node as the embedded traffic agent. Preferably, the embedded agent and NM agent pass data and commands between them and otherwise operate in coordination. Alternatively or

the user interface displays a topological picture of the network on which the user may indicate, using a pointing device, traffic agents to be used in a next step of the test, NM agents to be polled, hosts to be addressed, links or nodes to be enabled or disabled, etc. Preferably, a pop-up menu for each selected agent allows the user to define traffic and connection parameters including quality of service, traffic duration, traffic patterns, applications to be invoked, etc. Preferably, the user may also modify parameters of existing scripts.

Preferably, the user interface and/or the testing center software include definitions of groups of traffic agents and/or of network management agents, which allow subscripts to be easily sent to an entire group of agents. Such groups may include, for example, all of the NM agents coupled to switches and/or routers, all of the traffic agents located in a given physical area or in a given address range, all of the traffic agents associated with hosts performing specific functions, such as mail or file servers, or any arbitrary group chosen by the user. Preferably, an instruction in a script may send subscripts to a specified number of agents in a group rather than to the entire group. When such a number is stated, the testing center selects the recipient agents randomly or according to a predetermined rule. The predetermined rule may be a method to choose the most sparse units in terms of the network topology or a method to choose a concentrated group.

In some preferred embodiments of the present invention, a script includes commands establishing a connection at a specific standard of quality of service (QoS) and/or service level agreement (SLA) and instructing one or more of the network management agents along the connection to report to the testing center regarding data flow through the connection. The reports from the NM agents are preferably used to determine whether the QoS and/or SLA are achieved. Preferably, the testing center further determines the delay, data loss ratio and/or jitter of the transmitted data. If the results violate the contracted service level, the testing center executes a script which correlates the reports from multiple NM agents along the path to discover the specific misbehaving node. Alternatively or additionally, the testing center instructs, sequentially, embedded traffic agents associated with nodes along the connection path to form connections, and these connections are tested in order to find a link or path segment which is responsible for the service agreement violation.

There is therefore provided in accordance with a preferred embodiment of the present invention, a method for testing a network having a plurality of nodes, including sending commands to one or more traffic agents connected to the network and to at least one network management agent coupled to a respective node of the network, transmitting data from at least

Preferably, the method includes sending a command to a network management agent to change a traffic characteristic of the network at one or more of the plurality of nodes.

Preferably, changing the traffic characteristic includes altering the operability of a link of the network.

5        Preferably, evaluating the network information to assess the state of the network includes determining whether a first part of the network operates properly by disabling a second part of the network and transmitting the data through the first part while the second part is disabled.

10        Preferably, transmitting the data includes transmitting data according to a statistical transmission time pattern.

Alternatively or additionally, transmitting the data includes transmitting a request to establish a communication connection.

Preferably, transmitting the data includes transmitting data in accordance with a standard application protocol.

15        Preferably, evaluating the network information includes determining whether a fault in the network is in the application or in the network.

Preferably, transmitting the data includes transmitting at least one packet of data which includes one or more fields of test information.

20        Preferably, the test information includes a time stamp, a sequence number or a connection identification.

Preferably, the method includes receiving the transmitted data at one of the traffic agents and determining network-related performance information at the traffic agent which received the transmitted data responsive to the commands and the test information.

25        Preferably, evaluating the network information to assess the state of the network includes locating a network fault.

30        There is further provided in accordance with a preferred embodiment of the present invention, apparatus for testing a network having a plurality of nodes, including a plurality of traffic agents which generate and transmit data over the network, one or more network management agents coupled to respective nodes of the network, which determine network information at the node, and a testing center which sends commands to the plurality of traffic agents to generate and transmit the data and to the at least one network management agent to determine the network information, and which receives and evaluates the network information from the at least one network management agent so as to assess performance of the network.

**BRIEF DESCRIPTION OF THE DRAWINGS**

Fig. 1 is a schematic graph of a communication network with a testing system, in accordance with a preferred embodiment of the present invention;

Fig. 2 is a schematic block diagram of a traffic generator, in accordance with a preferred  
5 embodiment of the present invention;

Fig. 3 is a schematic block diagram of a traffic analyzer, in accordance with a preferred embodiment of the present invention;

Fig. 4 is a schematic block diagram of a testing center, in accordance with a preferred embodiment of the present invention;

10 Fig. 5 is a flow chart illustrating a sample test session, in accordance with a preferred embodiment of the present invention;

Fig. 6, is a schematic graph of a communication network, on which the sample test session of Fig. 5 is demonstrated; and

Fig. 7 is a schematic illustration of a graphical user interface (GUI) associated with the  
15 test center of Fig.4, in accordance with a preferred embodiment of the present invention.

hereinbelow, in order to test the network. Alternatively or additionally, testing system 22 comprises one or more combined traffic agents 64 which operate as both generators and analyzers. As indicated in Fig. 1, traffic agents 60, 62 and 64 may be implemented as part of hosts 36, either as additional hardware, such as add-on cards, or as software packages within the hosts. Although for most testing purposes, software packages are sufficient to implement traffic agents 60, 62 and 64, when network 20 is a very fast network, such as an ATM or a Gigabit Ethernet network, high-speed devices are required for full-scale testing of the network. Therefore, in such fast networks some or all of traffic agents 60, 62 and 64 preferably comprise add-on hardware devices.

Alternatively or additionally, end-point traffic agents 60, 62 and 64 may be implemented as stand-alone devices, independent of hosts 36. Such stand-alone agents may be used, for example, when special equipment is connected temporarily to network 20 for testing purposes. Preferably, system 22 also includes embedded traffic agents (EA) 67 which connect to switches 24 directly, not through a port 30. In all other aspects, embedded agents 67 are preferably the same as traffic agents 60, 62 or 64.

Testing system 22 further comprises one or more network management (NM) agents 70, which are associated with one or more of switches 24. For simplicity, NM agents 70 in Fig. 1 are not enclosed in the dashed line designating testing system 22. Preferably, network management agents 70 monitor, measure, and analyze the data and/or communication connections passing through the switches 24 to which they are coupled. NM agents 70 preferably have capturing and filtering capabilities which allow them to identify and/or count data packets from a specific link, or a specific origin, or data packets with specific properties. Further preferably, network management agents 70 include an RMON (Remote Monitoring) extension or other software or hardware extension which allows the network management agent to determine a profile of the data traffic through switch 24, including the amount of data headed to each different destination.

Preferably, network management agents 70 control components of their respective switches 24, most preferably by changing entries in configuration tables of the switch. Thus, for example, an NM agent 70 may activate or deactivate a link 26, change the queuing and/or the priority properties at the link, and/or change the quality of service (QoS) features of the respective switch 24 and its links.

Preferably, NM agents 70 comprise standard network management agents which are normally included in networks for interaction with NMS 58. Preferably, NM agents 70 include

the network, and/or test backup components which normally are not in use or are bypassed by the traffic.

Fig. 2 is a schematic block diagram of traffic generator 60, in accordance with a preferred embodiment of the present invention. The blocks in Fig. 2, which form traffic generator 60, are preferably software processes and/or subroutines which run on one of hosts 36. Preferably, the processes of traffic generator 60 may operate substantially concurrently. It is noted, however, that one skilled in the art will be able to implement a similar generator 60 in hardware.

Preferably, traffic generator 60 comprises an input interface 110 and an output interface 115 through which the traffic generator communicates with network 20. Alternatively, a single interface is used by generator 60 to communicate with network 20.

Traffic generator 60 preferably further comprises a command extractor 125 which is connected to interface 110 and recognizes commands from testing center 80 addressed to the generator. An execution module 100 receives the commands recognized by extractor 125 and determines the execution time of the commands. Commands without an execution time and/or condition are preferably carried out by the execution module immediately, while commands which have a condition or execution time are stored in a memory for further use. Preferably, a scheduler 105 continuously checks the times and conditions of the stored commands and initiates the execution of stored commands when appropriate.

In some preferred embodiments of the present invention, some of traffic generators 60 are included in a single, integrated, traffic agent 64, which includes a traffic analyzer 62. Such generators 60 preferably comprise an analyzer interface 120, which directly communicates with the respective analyzer 62. Thus, execution module 100 may receive commands and information directly from analyzer 62 and/or may pass commands directly to the analyzer. In this way, execution module 100 may generate responses to data received by analyzer 62 and/or send data on connections established with analyzer 62, all upon the initiative of a remote agent.

Generator 60 further comprises a packet generator 130 which generates packets (or cells in ATM networks) to be transmitted via output interface 115. Packet generator 130 generates data packets according to parameters of commands received by execution module 100. Preferably, the packets are generated according to a pattern or statistical profile defined in the command. Sample statistical profiles are described further hereinbelow.

Preferably, generator 130 generates the packets in two steps. In a first step, generator 130 prepares, responsive to a received command, entries in a generation table which comprises

specify the data to be generated and when the data are to be transmitted. A first command may order generation and transmission of a packet, a stream of packets or a plurality of streams of packets. Such a command may include parameters, such as the addresses of the receiving traffic analyzers and/or the number of bytes in each packet. This number may be fixed, or it  
5 may be set according to a predetermined pattern or a random pattern, in accordance with statistical settings which are pre-programmed or received in the command. The statistical settings may follow, for example, a geometric distribution. For example, the number of bytes in each packet may be formed of a fixed number of bytes including test information and a variable number of bytes including random data.

10 Similarly, the number of packets sent in a single stream and/or the time length of the stream are set according to one or more parameters. Preferably, the one or more parameters also determine the relative timing of the transmission of the packets in the stream, according to a statistical profile. For example, the packets may be transmitted according to a periodic, a Poisson and/or an ON-OFF model. The statistical profile is preferably chosen based on  
15 experimental measurements or records of actual network traffic monitored during normal network operation periods.

Further parameters may be used to set the contents of the packets, such as flags which indicate the beginning and end of a stream.

Other commands sent to generator 60 may instruct the generator to save the actual  
20 transmission data for further reference and/or to send the actual transmission data to testing center 80.

In connection-oriented networks, the commands to traffic generator 60 preferably include commands to generate connections, so as to allow testing of the ability of network  
25 to establish connections between hosts. A command for establishment of a connection (a "call" command) preferably states the number of connections, the times they are to be established, the hosts to connect to, the desired QoS, a list of variables in which the results of the connection establishment attempt are stored, etc.

Table 1 describes a taxonomy of commands for connection generation by traffic generators 60, in accordance with a preferred embodiment of the present invention.

30  
**Table 1**

Call:

Protocol:<description of connection protocol>

requests from network 20. Preferably, network interface 150 determines parameters of each of the received packets, which parameters may include arrival time, identity of the sending generator 60, packet type, packet length, sequence number and the dedicated test information in the payload section of the packet.

5        Preferably, in connection-oriented networks, network interface 150 may also determine the behavior of connection establishment requests arriving at analyzer 62.

Analyzer 62 preferably comprises a connection table 154 which contains, for each received connection or stream of packets, an entry which summarizes information pertaining to the connection or stream. Preferably, each entry includes information, such as the number of  
10    received packets in the stream, a total delay of the stream, a most recent reception time, an accumulated inter-packet timing, the number of lost packets, etc.

Preferably, table 154 includes entries only for connections or streams for which commands from testing center 80 have specifically requested analysis. Alternatively or additionally, table 154 may record substantially all of the received connections and a command  
15    from testing center 80 notifies analyzer 62 which connections to report.

The entries of table 154 are preferably identified by the reference number of the stream or connection. Alternatively or additionally, commands from testing center 80 may identify or limit the tracking of desired entries using one or more of the arrival time or transmittal time of the packets, the identity of the transmitting host, the route or a part thereof through which the  
20    packets are passed, the contents of the packets, or any other suitable variables.

Preferably, for connections in connection-oriented networks, table 154 summarizes information regarding the connection, such as connection and termination activities, the number of established connections and their final negotiated parameters, the time at which they were received and the inter-call timing. A second copy of this information may reside on the other  
25    traffic agent participating in the connection.

A finite state machine 152, preferably implemented by software, updates the entries in table 154 based on the parameters of the received packets. In addition, finite state machine 152 preferably signals a command execution module 156 when a last packet of a stream has been accepted. The last packet in the stream may be identified according to a flag in the packet, or  
30    according to an identity number or time stamp of the packet beyond the required range to be tracked. Preferably, a mapping table 160 may be used by finite state machine 152 to access table 154.

Execution module 156 preferably receives commands from testing center 80 and

and/or altered by the operator.

Preferably, testing center 80 comprises a memory library 88 in which instruction scripts for various test sessions are stored. Testing center 80 may automatically perform a test session according to a script stored in library 88, periodically and/or in response to one or more  
 5 conditions of network 20, such as in response to alarms generated by network management system 58. Alternatively or additionally, the operator may invoke one or more scripts in library 88.

Preferably, before automatically initiating a test session, testing center 80 checks the traffic volume through certain nodes in the network, preferably by probing NM agents 70. If  
 10 the volume is relatively high, the test is preferably deferred to a later time so that the test will not interfere with operation of the network. Alternatively or additionally, the script of the automatic test session varies responsive to the traffic volume of the network. Preferably, the traffic volume is periodically assessed during relatively long test sessions to prevent any adverse influences of a long test on traffic which appeared after the test began. Preferably, the testing of  
 15 the traffic is included in a script which is invoked by other scripts as required.

Testing center 80 preferably comprises a communication adapter 90 (for example, an Ethernet card), through which the testing center communicates with traffic agents 60, 62 and 64 and network management agents 70. Testing center 80 preferably communicates with the agents using a standard protocol, such as the TCP/IP protocol suite.

20 Table 2 describes a taxonomy of a transmission instruction included in scripts stored in memory library 88, in accordance with a preferred embodiment of the present invention. The transmission instruction causes testing center 80 to send a subscript to one or more of traffic agents 60, 62, 64 and 67.

25 Table 2

Send\_Command [-options]  
 [#At: date and time]  
 #To: <list of recipient traffic agents>  
 #Command\_reference\_number <number>  
 30 [#Type: command\_type]  
 #Data: [pointer]  
 [subscript]  
 #End of Data

the descriptions of the traffic agents 60 and 62. Alternatively or additionally, the general taxonomy of the commands is in accordance with standards known in the art, such as UNIX shell, tcl/tk, SNMP, Java Script macros, etc.

Fig. 5 is a flow chart illustrating a sample test session, in accordance with a preferred embodiment of the present invention. Reference is also made to Fig. 6, which is a schematic graph of a communication network 190, on which the sample test session is demonstrated. Preferably, the sample test session is implemented by invoking a script stored in memory library 88. Network 190 comprises an ATM standard network in which all the communication links operate at 155 Mbps.

As indicated in block 170, traffic generators 250, 252 and 254 are instructed to establish connections with traffic analyzer 272. Preferably, traffic generators 250, 252 and 254 are instructed to report to testing center 80 when the connections are established. Preferably, a connection is also established between generator 252 and analyzer 270. Preferably, analyzers 270 and 272 are instructed to accept the requests for connection establishment. After about 30 seconds, traffic generator 250 is instructed to generate a stream of packets according to a Poisson random process, at an average rate of 50 Mbps. The stream is sent to analyzer 272, which is instructed to track the stream and report intermediate data flow results to testing center 80 approximately once every 20 seconds.

About 20 seconds later, traffic generator 254 is instructed to generate a stream at a constant rate of 60 Mbps and send the stream to analyzer 272. This stream is also tracked by analyzer 272. After another 20 seconds, generator 252 is instructed to produce an ON-OFF traffic transmission process with an ON period comprising 20% of its total time, at an average rate of 50 Mbps. Preferably, this stream is not tracked and only serves to load network 190 such that the network may be tested with a high load.

Preferably, generator 252 is instructed to send another stream, such as a modulated Poisson source behavior stream, to analyzer 270. The stream preferably has three equal probability states, having transmission rates of 10, 20 and 30 Mbps, each state having an average duration time of 0.1 seconds. Analyzer 270 is preferably instructed to track this stream.

Preferably, during the entire test session, each of switches 204, 206, 208 and 212 is instructed to report periodically on the data flow through the switch.

After a predetermined amount of time, preferably between about 2 and 5 minutes, all of the streams are terminated and testing center 80 receives all of the data from switches 204, 206, 208 and 212 and analyzers 270 and 272. Testing center 80 preferably summarizes the data on

60, and an NM icon 370 represents an NM agent 70. Preferably, links 26 are represented by lines 372. Preferably, operator 96 can use clicking and drag and drop operations upon the map blocks in order to design and build new test scripts or determine the parameters of a test script contained in library 88. Preferably, the GUI includes a test library list 320 which lists all the  
5 available tests in library 88. Preferably, list 320 is sorted and grouped according to various cuts that allow easy access of operator 96 to the scripts in library 88. Preferably, operator 96 accesses a script by clicking on a pull down icon 322, as is known in the art.

Preferably, upon clicking on the blocks of network map 310, respective windows open which allow setting parameters of test scripts. For example, upon clicking on traffic icon 330, a  
10 traffic agent window 340 pops up with proper fields for entering parameters of instructions of the scripts. Such fields include, for example, a transmit field 350 and a receive field 360 for inputting respective parameters of the scripts. Preferably, the parameters of transmit field 350 include fields which indicate the type of the transmitted stream, e.g., Poisson, and its rate, e.g.,  
15 10 Mb/s. The parameters of receive field 360 include a list of variables to be measured, e.g., delay. Preferably, fields 350 and 360 include start and stop buttons 352 which are used to begin and end transmission of traffic streams. Alternatively or additionally, other icons may be used to indicate the timing of the streams. Preferably, upon clicking on NM icon 370, a network management window 380 opens with fields for setting parameters related to the NM agent represented by icon 370. The network management window 380 preferably includes a  
20 monitoring field 382 which is used to set monitoring parameters, such as the source of traffic to be monitored, and a configuration field 384, which is used to change the configuration of network 20, e.g., enable and disable links of the network.

Preferably, the GUI also includes fields which display the test results in various forms such as a condensed or a detailed summary of the results of the test, or presenting the results  
25 using graphical tools.

In some preferred embodiments of the present invention, testing system 22 comprises more than one testing center 80. Preferably, each testing center sends instructions to and receives reports from a group of traffic agents. Preferably, the groups of traffic agents are exclusive, and one traffic agent does not receive instructions from more than one testing center  
30 80. Alternatively or additionally, each testing center 80 may send instructions to and receive reports from every traffic agent. Preferably, one of the testing centers 80 sends instructions to and receives reports from the rest of the testing centers.

It will be appreciated that the preferred embodiments described above are cited by way

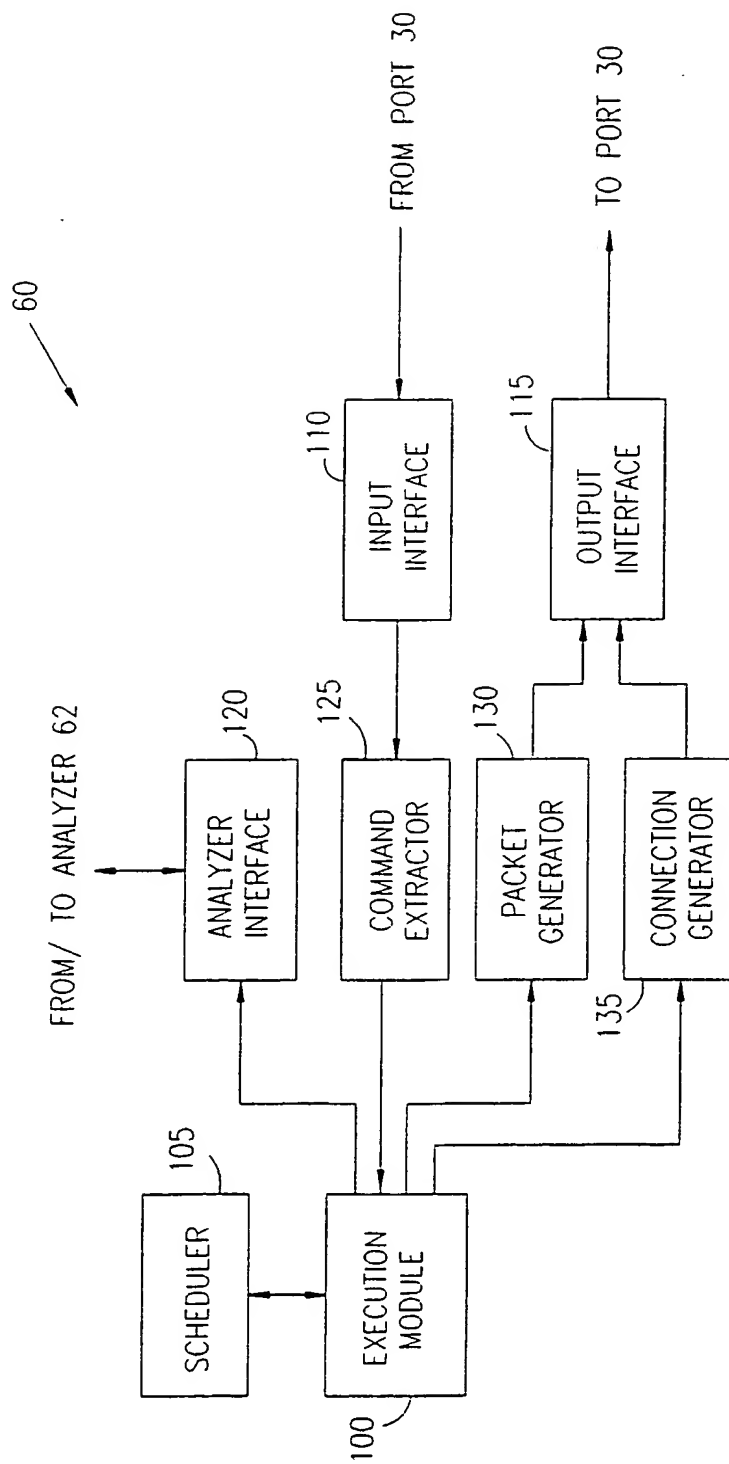
## CLAIMS

1. A method for testing a network having a plurality of nodes, comprising:  
sending commands to one or more traffic agents connected to the network and to at least one network management agent coupled to a respective node of the network;  
5 transmitting data from at least one of the traffic agents over the network responsive to the commands;  
determining network information at the at least one network management agent responsive to the commands and to transmission of the data through the respective node; and  
receiving and evaluating the network information to assess a state of the network.  
10
2. A method according to claim 1, wherein sending the commands comprises sending commands to the one or more traffic agents and to the at least one network management agent from a single source.
- 15 3. A method according to claim 1, wherein sending the commands comprises sending commands over the network.
4. A method according to claim 1, and comprising receiving at least some of the transmitted data in at least one of the traffic agents and deriving additional network information  
20 at the traffic agent which received the data, responsive to the commands.
5. A method according to claim 4, wherein deriving the additional network information comprises determining a response time property of the transmitted data.
- 25 6. A method according to claim 1, wherein determining network information comprises capturing data transmitted by at least one of the plurality of the traffic agents.
7. A method according to claim 1, wherein transmitting the data comprises multicasting the data.  
30
8. A method according to claim 1, wherein sending the commands comprises sending a pre-stored subscript of commands.

19. A method according to claim 18, wherein changing the traffic characteristic comprises altering the operability of a link of the network.
- 5 20. A method according to claim 19, wherein evaluating the network information to assess the state of the network comprises determining whether a first part of the network operates properly by disabling a second part of the network and transmitting the data through the first part while the second part is disabled.
- 10 21. A method according to any of claims 1-17, wherein transmitting the data comprises transmitting data according to a statistical transmission time pattern.
22. A method according to any of claims 1-17, wherein transmitting the data comprises transmitting a request to establish a communication connection.
- 15 23. A method according to any of claims 1-17, wherein transmitting the data comprises transmitting data in accordance with a standard application protocol.
24. A method according to claim 23, wherein evaluating the network information comprises  
20 determining whether a fault in the network is in the application or in the network.
25. A method according to any of claims 1-17, wherein transmitting the data comprises transmitting at least one packet of data which includes one or more fields of test information.
- 25 26. A method according to claim 25, wherein the test information comprises a time stamp, a sequence number or a connection identification.
27. A method according to claim 25, and comprising receiving the transmitted data at one of the traffic agents and determining network-related performance information at the traffic  
30 agent which received the transmitted data responsive to the commands and the test information.
28. A method according to any of claims 1-17, wherein evaluating the network information to assess the state of the network comprises locating a network fault.

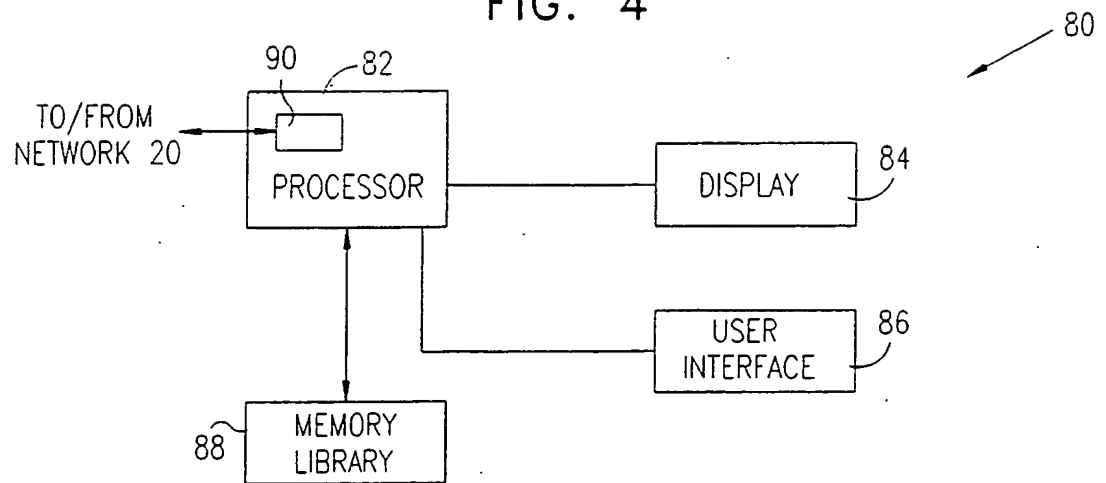
37. Apparatus according to claim 36, wherein the user interface comprises a graphical user interface which allows a user to create some or all of the scripts.
38. Apparatus according to claim 37, wherein the graphic user interface allows the user to  
5 change parameters of the scripts.
39. Apparatus according to claim 29, wherein at least one of the network management agents changes a traffic characteristic of the network responsive to the commands.
- 10 40. Apparatus according to claim 39, wherein the at least one of the network management agents alters the operability of a link of the network.
41. Apparatus according to any of claims 29-40, wherein the at least one of the network management agents captures the transmitted data.
- 15 42. Apparatus according to any of claims 29-40, wherein the network management agent comprises a Remote Monitoring agent.
43. Apparatus according to any of claims 29-40, wherein the plurality of traffic agents  
20 comprise at least one traffic agent which is internal to a node of the network.
44. Apparatus according to any of claims 29-40, wherein the plurality of traffic agents comprise at least one traffic agent which is implemented as an integral part of one of the network management agents.

FIG. 2



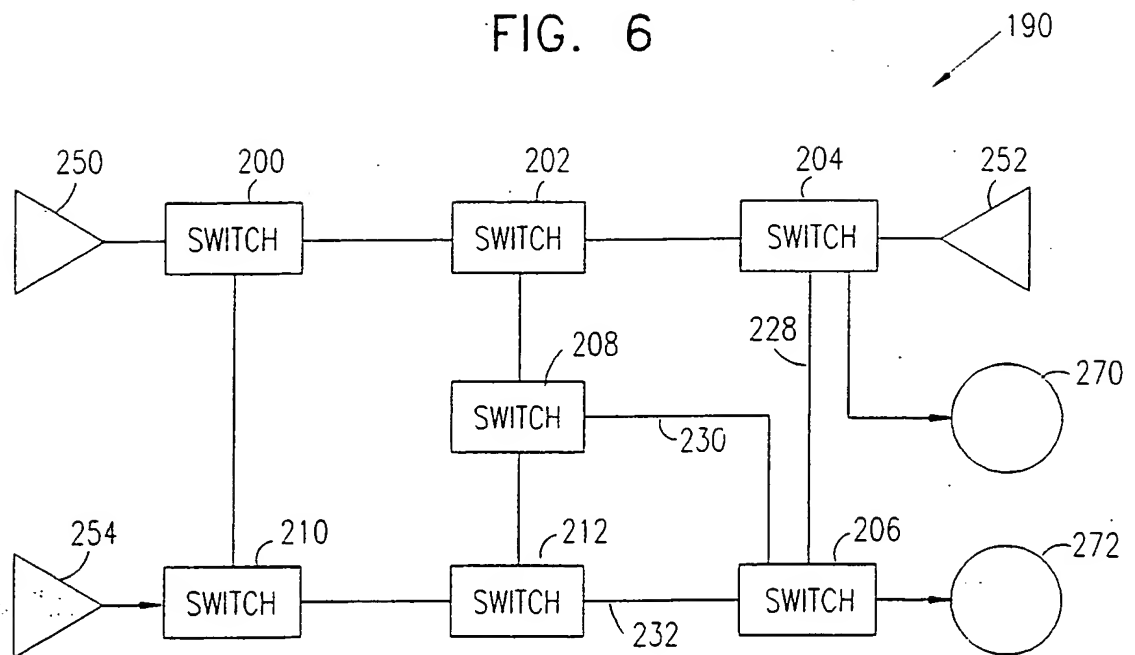
4/7

FIG. 4



6/7

FIG. 6



# INTERNATIONAL SEARCH REPORT

International Application No

PCT/IL 98/00475

**A. CLASSIFICATION OF SUBJECT MATTER**  
IPC 6 H04L12/26 H04L12/24

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	KEISER G ET AL: "Test traffic generation equipment and algorithms for evaluating ATM networks"	1-6, 8, 11, 16, 21, 23, 29-31, 41
A	COMPUTER COMMUNICATIONS, vol. 19, no. 12, October 1996, page 962-971 XP004052780 see the whole document	7, 9, 10, 12-15, 17-20, 22, 24-28, 32-40, 42-44
	--- -/--	

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

\* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"Z" document member of the same patent family

Date of the actual completion of the international search

11 January 1999

Date of mailing of the international search report

21/01/1999

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Authorized officer

Cichra, M

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/IL 98/00475

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9607281 A	07-03-1996	AU 3393595 A	22-03-1996
		CA 2198885 A	07-03-1996
		EP 0786187 A	30-07-1997
		FI 970849 A	25-04-1997
		JP 10504949 T	12-05-1998
		NO 970943 A	28-04-1997
		NZ 292213 A	26-05-1997
<hr/>			